Предисловие.

Сегодняшние реалии в развитии современных информационных систем (ИС) таковы: они становятся всё сложнее, их эксплуатация всё дороже. Как следствие, всё острее встаёт проблема повышения эффективности, достоверности и скорости принятия решений по локализации и диагностике при проявлении дефектов ИС в ходе её эксплуатации, и, наконец, в скорости выработки управленческих воздействий на эксплуатируемую систему. Решение проблемы лежит в автоматизации наиболее рутинных и трудоёмких процессов обеспечения эксплуатации современных ИС. Но, говоря об автоматизации, мы вынуждены искать способы повышения её эффективности. Современные тенденции в этой области – это использование средств интеллектуализации обработки данных о функционировании ИС с целью повышения эффективности принятия решений в процессах эксплуатации ИС, и в частности, в использовании автоматизированных систем, основанных на знаниях. Любой сбой в ИС, любой факт нарушения её функциональности, зафиксированные и соответствущим образом оформленные специалистами службы эксплуатации, уже есть знания. Но, знания необходимо уметь извлекать, фиксировать, как-то систематизировать, хранить, обеспечивать к ним доступ и обрабатывать. И это является, по сути, целым набором технологических проблем, требующих отдельных специализированных решений, последовательно раскрываемых в данной книге. Применительно к рассматривамой проблеме повышения эффективности принятия решений по совершенствованию процессов эксплуатации современных ИС, любое решение основывается на знаниях об объекте ИС, которым, в зависимости от состава и характера решаемых задач, может являться системное или прикладное программное обеспечение или отдельный модуль в их составе, сетевое оборудование ИС и его компоненты, структуры данных и сами данные. Такие знания, используемые в ходе эксплуатации ИС, делятся на две группы: *нормативные*, - описывающие штатный режим работы ее компонентов на основании различных справочников, а также технической и эксплуатационной документации, и *уникальные*, - получаемые в результате разрешения инцидентов[1], возникающих непосредственно в процессе эксплуатации. Использование нормативных знаний в большинстве случаев не позволяет учитывать и оперативно обрабатывать различные аспекты взаимодействия конкретных аппаратных и программных компонентов в составе действующей ИС. Уникальные знания, накопленные в процессе эксплуатации ИС, также

[1] Под инцидентами здесь подразумеваются любые события, оказывающие отрицательное воздействие на нормальное (штатное) функционирование подсистемы или сервиса ИС [11].

называемые экспертными знаниями[2], обладают большей ценностью, однако, из-за отсутствия эффективных инструментальных средств их фиксации – приобретения, обработки и накопления с целью последующего использования, возможность их широкого применения ограничена. Таким образом, центральной проблемой создания таких автоматизированных систем, основанных на знаниях, остаётся разработка инструментарного прикладного программного обеспечения, обеспечивающего решение конкретных задач повышения эффективности принятия решений в процессах эксплуатации ИС. При этом эффективность таких инструментов определяется не столько их производительностью, сколько удобством их функционального развития, способностью к эволюции, и в частности, - устойчивостью к изменениям эксплуатируемой ИС в течение жизненного цикла. Сам факт перехода на новую технологическую парадигму повышения эффективности, достоверности и скорости принятия решений по локализации и диагностике при проявлении дефектов ИС в ходе её эксплуатации, с использованием автоматизированных систем, основанных на знаниях, закономерен, однако, ситуация при этом зачастую оказывается не вполне благоприятной для разработчиков подобных инструментальных систем и их потребителей в силу следующих основных причин.

1. *Существование.* На рынке инструментарного прикладного программного обеспечения, обеспечивающего решение целого ряда задач повышения эффективности принятия решений в процессах эксплуатации ИС, существует некоторый набор программных инструментальных средств, в разной степени использующих поход, основанный на использовании баз экспертных знаний, которые можно отнести к одному трёх типов – инцидентов, проблем и их решений, и библиотек справочных и информационно-аналитических материалов. Каждый программный инструмент подразумевает использование базы знаний, как правило, одного типа.

2. *Отсутствие.* Эффективность использования таких инструментов имеет весьма низкий уровень, вследствии отсутствия оснований их функциональной интеграции, а именно: отсутствия внятной системы классификации инцидентов для формирования баз знаний *первого* типа, отсутствия информации о причинно-следственных связях для всех инцидентов, вызванных какой-то проблемой, - для формирования баз знаний *второго* типа, и наконец, - отсутствия механизма создания и поддержания в актуальном состоянии связей между записями в базах данных инцидентов и проблем, а также - в базах знаний *третьего* типа.

3. *Формализация.* Для создания такого инструментарного прикладного программного обеспечения, позволяющего интегрировать функциональность баз знаний трёх типов необходим соответствующий аппарат формализации и

[2]Основой их формирования являются, как правило, эксперты – высокопрофессиональные специалисты в области эксплуатации и поддержки функциональности современных ИС.

классификации экспертных знаний в данной предметной области – автоматизированные интеллектуальные системы повышения эффективности принятия решений в процессах эксплуатации ИС, основанные на знаниях.

Программные инструменты повышения эффективности принятия решений в процессах эксплуатации ИС, события и инциденты, базы экспертных знаний, онтологии экспертных знаний, классификация инцидентов составляют основное содержание книги. В книге не предполагается детально рассматривать конкретные реализации используемых подходов для практических реализаций в построении подобных программных инструментов и их компонентов. Подобный анализ явился предметом ряда аналитических материалов, опубликованных в России [2, 8, 15-17, 29, 33] и за рубежом [47, 48-50]. Принимая во внимание это обстоятельство, в начале книги дана лишь общая характеристика баз экспертных знаний и инцидентов, как объектов их содержимого, экспертных баз проблем и их решений, и экспертных баз библиотек справочных и информационно-аналитических материалов. Основная же часть книги посвящена описанию применения и проектирования онтологического подхода для формализации и организации баз экспертных знаний в предметной области обработки инцидентов в ИС. Структурирование экспертных знаний предметной области обработки инцидентов в ИС осуществляется с помощью двух независимых классификаторов инцидентов. Применение онтологического подхода и предложенных классификаторов инцидентов позволило разработать концептуальную и математическую модели представления знаний об инцидентах в ИС, на основе которых разработано прикладное программное обеспечение инструментария.

В книге принят следующий порядок изложения. В *первой главе* выполнен анализ программных инструментов организации баз экспертных знаний, полученных при обработке инцидентов в ИС. Предложены критерии сравнения существующих подходов и программных инструментов, включающие в себя используемый формат хранения данных, способы и источники наполнения баз знаний, наличие предустановленных шаблонов и записей о типовых инцидентах, наличие механизма создания и поддержания причинно-следственных связей между соответствующими записями в базах знаний, возможность интеграции с ресурсами сторонних поставщиков. На основании данных критериев проведен сравнительный анализ программных инструментов ряда производителей.

Типовым решением является раздельное хранение собранной информации в базах данных инцидентов, проблем и их решений, предназначенных преимущественно для специалистов службы технической поддержки (СТП). При этом подробное описание способа разрешения в записи об инциденте в большинстве случаев не приводится. Базы данных проблем, напротив, содержат подробное описание корневых причин

возникновения инцидентов и способов их разрешения, но не содержат информации обо всех инцидентах, вызванных той или иной проблемой.

Другим стандартным инструментом являются базы знаний, представляющие собой библиотеки информационно-аналитических статей, содержащих слабоструктурированную информацию, как правило, разрозненных.

Общим недостатком существующих программных инструментов является отсутствие механизма создания и поддержания в актуальном состоянии связей между записями в базах данных инцидентов и проблем, а также в имеющихся информационных базах знаний. Существующие программные инструменты не позволяют администратору ИС видеть причинно-следственные связи между событиями, приводящими к нарушению функционирования ИС, или по запросу получать ответ на следующие группы вопросов: какие ранее возникшие инциденты и проблемы могли привести к возникновению данного инцидента, сколько зарегистрированных инцидентов связано с отдельно взятым объектом в составе ИС или к возникновению каких инцидентов может привести известная проблема.

Во *второй главе* проведено исследование возможности применения онтологического подхода для формализации и организации баз экспертных знаний в предметной области обработки инцидентов в ИС, при котором знания, накопленные в ходе эксплуатации ИС, организуются в виде таксономии, описывающей иерархическую систему понятий, связанных друг с другом отношениями с определенной семантикой, что позволяет структурно организовывать сущности в составе онтологии в виде графа. В общем случае таксономия объектов предметной области включает в себя следующие элементы:

- *понятия-сущности*, соответствующие значимым объектам рассматриваемой области деятельности;
- *понятия-отношения*, соответствующие связям между объектами;
- *понятия-свойства*, описывающие значимые параметры и характеристики объектов или их отношений.

В результате, использование двух независимых классификаторов для структурирования знаний предметной области обработки инцидентов в ИС позволяет, в зависимости от специфики решаемых задач:

- получать подмножество инцидентов, связанных с заданным объектом, и последовательно, в соответствии с распределением по уровням модели ISO/OSI, просматривать их;

- выбирать нужный уровень модели для указанной подсистемы или компонента ИС, после чего просматривать полученное подмножество инцидентов для нахождения связанных с искомым объектом.

Применение онтологического подхода и предложенных классификаторов инцидентов позволило разработать концептуальную и математическую модели представления знаний об инцидентах в ИС.

В зависимости от порядка просмотра уровней, модель позволяет получать подмножества инцидентов, связанных с заданным объектом (прямой порядок «сверху-вниз»), или определять подмножество объектов, связанных с выбранным инцидентом (обратный порядок «снизу-вверх»). База экспертных знаний, организованная с использованием предложенной математической модели, содержащей, в том числе, формальное определение инцидента, позволяет описывать все доступное множество объектов и инцидентов - содержит все необходимые знания для обработки инцидентов, возникающих в ИС.

В *третьей главе* сформулированы требования, предъявляемые к подобным программным инструментальным средствам в соответствии с полученными ранее моделями представления знаний об инцидентах в ИС. В их число входят как архитектурные – возможность реализации в виде standalone-приложения и Java-апплета, поддержка внешних источников данных, так и обусловленные спецификой используемого подхода – поддержка логической организации сущностей и отношений в соответствии с разработанными методами классификации и структурирования знаний об инцидентах в ИС.

Для реализации действующего прототипа выбран комплект средств разработки на основе свободного ПО Thinkmap SDK, предназначенный для создания прикладных программ, решающих задачу обработки и визуализации больших объемов данных.

В соответствии с описываемыми концептуальной моделью свойствами сущностей и отношений, определены соответствующие структуры данных. В книге они используются для описания в формате XML шести типов понятий-сущностей, четырех типов иерархических и двух типов специфических для предметной области понятий-отношений, включенных в ранее описанную таксономию объектов.

Все объекты, обрабатываемые и визуализируемые с помощью разработанной системы, представляются в виде графовой модели. В каждый момент времени пользователю доступно определенное подмножество объектов (фрагмент графовой модели) с возможностью перехода к новому подмножеству при необходимости. Такое подмножество, выбранное на основе значений указанных параметров, рассматривается в данной книге как представление. Для построения представлений (отбора всех входящих в них объектов и связей между ними) предложены специальные условия обхода

графа, реализованные с использованием инструментального средства разработки Thinkmap SDK.

С позиции онтологического подхода, данная операция аналогична поиску термина, представляющего интерес для решения определенной задачи, и формирования соответствующего контекста. Под контекстом здесь подразумевается часть (срез) онтологии, значимая для ее решения.

В *четвертой главе* приведены результаты апробации разработанного программного инструментария приобретения и представления экспертных знаний, выполненной в процессе эксплуатации программно-аппаратного комплекса Федерального центра информационно-образовательных ресурсов [53].

В книге приведены примеры записей в базе знаний, созданных средствами программного инструментария в ходе опытной эксплуатации, а также количественные показатели для таких параметров, как число зафиксированных инцидентов, описанных объектов и ряда других в соответствии с разработанной концептуальной моделью представления знаний об инцидентах в ИС.

Проверка целостности и непротиворечивости базы экспертных знаний после ее информационного наполнения средствами разработанной системы выполнена с использованием среды Protégé, для чего XML-описание разработанной ранее таксономии объектов было преобразовано в соответствии со стандартами языка описания онтологий OWL [67]. Дано описание основных структурных элементов полученной OWL-онтологии и их соответствие элементам таксономии объектов; приведены основные этапы построения OWL-онтологии; представлены примеры выполнения специальных запросов, построенных в соответствии с синтаксисом OWL к разработанной онтологии.

Для определения соответствия разработанной системы приобретения и представления экспертных знаний сформулированным функциональным требованиям приведена программа испытаний, включающая в себя различные сценарии ее использования. Состав, порядок и методика проведения испытаний приведены в приложении В.

Для оценки эффективности разработанного инструментария применен подход определения количественных мер измерения – метрик – значимых параметров, предлагаемых методологией ITSM. Оценка эффективности проводилась на основании таких метрик, как процент инцидентов, решенных на первой линии поддержки или проактивно, а также как среднее время разрешения и общее число инцидентов, разрешенных с использованием экспертных знаний, содержащихся в полученной базе знаний.

Общая оценка повышения эффективности выполнена на основе расчета интегрального показателя, учитывающего значения перечисленных метрик и приоритетов, определяющих степень их значимости в целом.

Увеличение значений метрик, определяющих положительные факторы при разрешении инцидентов в ИС с использованием разработанной базы знаний – точность первоначальной классификации, правильность и скорость их разрешения, а также уменьшение значений метрик, оценивающих негативные факторы, – невозможность определить корневую причину возникновения, неверную классификацию, и, как следствие – рост интегрального показателя в целом, подтверждают возможность использования системы приобретения и представления экспертных знаний для достижения поставленной цели.

В Заключении определены направления дальнейшего развития работ в развитие данного подхода.

Введение

Знания, используемые в ходе эксплуатации ИС, делятся на две группы: *нормативные*, описывающие штатный режим работы ее компонентов на основании технической и эксплуатационной документации, а также различных справочников, и *уникальные*, получаемые в результате разрешения инцидентов[3], возникающих непосредственно в процессе эксплуатации. Использование нормативных знаний в большинстве случаев не позволяет учесть различные аспекты взаимодействия конкретных аппаратных и программных компонентов в составе действующей ИС. Уникальные знания, накопленные в процессе эксплуатации ИС, также называемые экспертными знаниями, с этой точки зрения обладают большей ценностью. Однако, из-за отсутствия эффективных инструментальных средств фиксации – приобретения, обработки и накопления с целью последующего использования – возможность их применения ограничена.

В настоящее время на рынке прикладного программного обеспечения не существует интегрированных инструментов организации баз экспертных знаний и их наполнения, предоставляющих реализацию концепции единой точки доступа ко всему объему знаний, накопленных в ходе создания и эксплуатации информационной системы. Это приводит к снижению эффективности решений, принимаемых в ходе эксплуатации ИС, в том числе, при разрешении возникающих инцидентов. Релизация механизмов обеспечения интегрированности предполагает наличие механизмов, обеспечивающих ирформационную связность содержимого баз экспертных знаний трёх типов: инцидентов, проблем и их решений, библиотек справочных и информационно-аналитических материалов. Эффективность, при этом, зависит как от качества данной информациии (базы экспертных

[3] Под инцидентами здесь подразумеваются любые события, оказывающие отрицательное воздействие на нормальное (штатное) функционирование подсистемы или сервиса ИС [11].

знаний, содержащие информацию об ицидентах), количества источников доступной информации (внутренние руководства аппаратного обеспечения, справочные системы программного обеспечения, справочные руководства по операциям, конфигурационные базы данных, системы обработки изменений и запросов пользователей, а также базы данных и библиотеки информационных статей службы технической поддержки, пособия системного администратора, документация по процессам), так и от квалификации специалистов. Но, информация данного рода на практике является, как правило, своего рода - закрытой, то есть охраняемой корпоративными интересами, поэтому практически не публикуется в открытых источниках. Библиотека ITIL [47-49] зачастую дает мало полезного в решении повседневных типовых задач сегодняшних служб технической поддержки, так как процессы ITIL описываются на более высоком уровне абстракции. С этой точки зрения данная книга является, с одной стороны, примером иллюстрации практического решения типовой задачи СТП – разрешения инцидентов, в части использования соответствующего программного инструментария, а с другой – её изложение построено на основе строгого системного подхода, в основе которого находятся классификация и онтология.

Целью монографии является описание процесса разработки и использования программного инструментария, позволяющего повысить эффективность, достоверность и скорость принятия решений по локализации и диагностике при проявлении дефектов ИС в ходе её эксплуатации на основе использования знаний о нарушении функциональности ИС, представленных в виде инцидентов. По сути, в терминологии ITIL, речь идёт об описании всего процесса создания и использования базы данных управления инцидентами IMDB (Incident Management Database).

В книге представлены решения следующих задач:

1. Разработка методов классификации и структурирования знаний об инцидентах в ИС (*на основе применения структурного подхода и эталонной модели взаимодействия открытых систем ISO/OSI).*
2. Разработка математических моделей и методов формализации экспертных знаний об инцидентах в ИС.
3. Разработка онтологии инцидентов в ИС (*на основе предложенных методов и моделей).*
4. Разработка программного инструментария для организации и наполнения базы экспертных знаний об инцидентах в ИС.
5. Апробация программного инструментария приобретения и представления экспертных знаний об инцидентах в ИС.
6. Определение количественных показателей повышения эффективности использования разработанного инструментария.